

REMARKS

Claims 1, 3, and 5-10 remain rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al. (US 6,327,661; hereinafter “Kocher”).

Applicant respectfully traverses this rejection.

Independent claim 3 recites “A digital integrated circuit comprising: ... means for time-varying a supply voltage of said asynchronous circuit to time-shift the execution point of operations within said asynchronous circuit ...”

Kocher discloses a noise production system 100 having a noise production module 105 configured to sink power, produce electromagnetic radiation, or otherwise introduce noise into attackers’ measurements. See Kocher, column 5, lines 22-29.

Kocher does not disclose varying a *supply voltage* to time-shift the execution point of operations, as required by independent claim 3. Kocher discloses that noise production system 100 sink’s power. The term “power” is not the same as “voltage”, and is certainly not the same as a “supply voltage”.

Further, Kocher does not disclose time-shifting operations within an asynchronous circuit, also required by independent claim 3. In rejecting this feature the Examiner refers to Kocher’s disclosure in column 5, lines 57-60, of clocking noise production modules independently. Applicant respectfully disagrees with the Examiner’s position. Kocher’s noise production modules do not correlate with the claimed asynchronous circuit. For the sake of argument, if one were to attempt to correlate the claimed subject matter with the disclosure of Kocher, the claimed means for time-varying a supply voltage might correlate with Kocher’s noise production module 100, and the claimed asynchronous circuit might correlate with Kocher’s microprocessor (225 in Figure 3; not shown in Figure 2). Kocher does not disclose time-shifting operations within the microprocessor.

Even further, Kocher does not disclose time-varying a supply voltage of an *asynchronous circuit* using a random number generator, as also required by independent 3. In rejecting this

asynchronous circuit feature, the Examiner refers to the UART (universal asynchronous receiver/transmitter) disclosed in Kocher at column 9, line 4. This portion of Kocher is directed to the embodiment involving clock skipping, not the embodiment involving random noise generation. There is no disclosure or even suggestion in Kocher of time-varying a supply voltage of this UART using a random number generator.

Kocher, column 7, lines 19-34, does not discuss clock skipping in relation to random noise generation, as the Examiner asserts. This portion of Kocher discloses only a “random number generator 200” which is used to determine which clock cycles are to be used by the microprocessor core 225. While random number generators may be used to generate random noise, disclosure of a random number generator is not the same as disclosure of random noise generation.

An “asynchronous circuit”, as is well known, is a circuit in which the components are largely autonomous. They are not governed by a clock circuit or global clock signal, but instead need only wait for the signals that indicate completion of instructions and operations.

Kocher in column 7, lines 6-15, discloses that clock skipping involves decorrelating cryptographic operations from the external clock cycles by creating a separate, internal clock signal that is used to control processor timing during cryptographic operations. An internal clock internal clock signal is used to control processor timing. There is therefore no disclosure that this control processor is an asynchronous circuit.

Independent claim 3 is therefore patentable over Kocher for at least these reasons.

Since independent claim 1 includes limitations similar to the limitation discussed above with respect to independent claim 3, it is patentable over Kocher for at least the same reasons.

Claims 5-10 depend from the independent claims, and are therefore patentable over Kocher for at least the same reasons.


Reconsideration and withdrawal of the prior art rejection are respectfully requested.

Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: May 12, 2011

Respectfully submitted,

By 

Laura C. Brutman

Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant